

(12) UK Patent Application (19) GB (11) 2 369 800 (13) A

(43) Date of A Publication 12.06.2002

(21) Application No 0030056.6

(22) Date of Filing 08.12.2000

(71) Applicant(s)
Consignia Plc.
(Incorporated in the United Kingdom)
148 Old Street, LONDON, EC1V 9HQ, United Kingdom

(72) Inventor(s)
Virginia Kate Pitts
James Ballantyne

(74) Agent and/or Address for Service
R.G.C. Jenkins & Co
26 Caxton Street, LONDON, SW1H 0RJ,
United Kingdom

(51) INT CL⁷
B42D 15/10 // B42D 115:00

(52) UK CL (Edition T)
B6A AC43 AK

(56) Documents Cited
GB 2314527 A **GB 2252270 A**
WO 98/43825 A1 **US 5577109 A**

(58) Field of Search
INT CL⁷ B42D 15/10 , G06K 19/00
Online databases: EPODOC, JAPIO, WPI

(54) Abstract Title
Cash card with scratch off surfaces

(57) A cash card 10 that is representative of a cash amount bears a unique identification number 14 and a unique validation number 18 that are concealed by removable scratch off surfaces 12,16. The validation number may be generated from the identification number using a one time pad. The card may be validated by a vendor of goods or services by checking the identification number with a computer database in which case a voice response unit provides the vendor with the validation number which can be checked with that on the card.

Figure 1

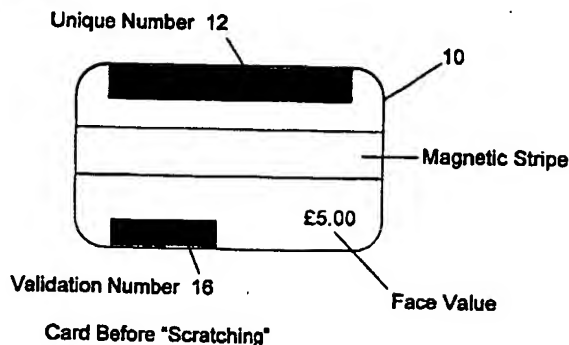


Figure 2

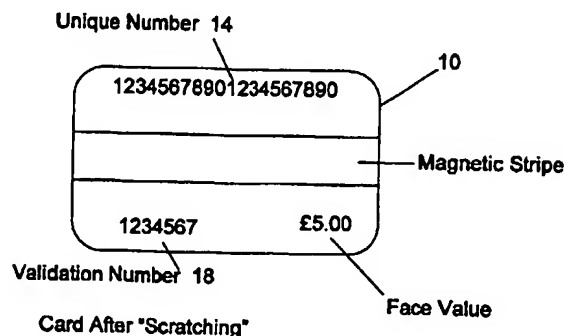
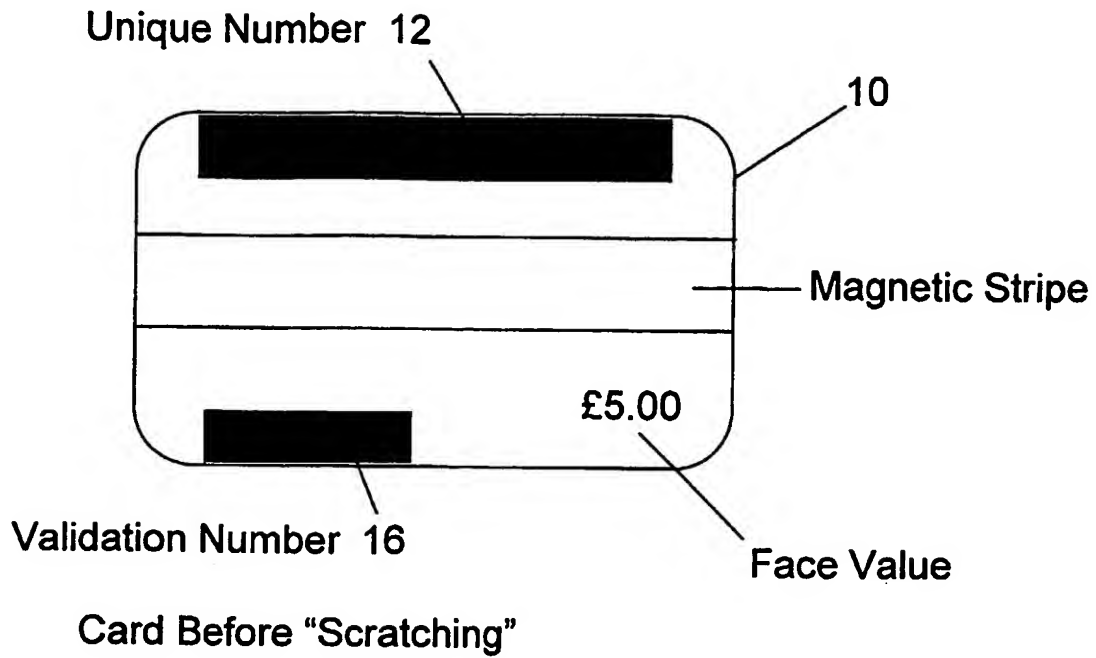
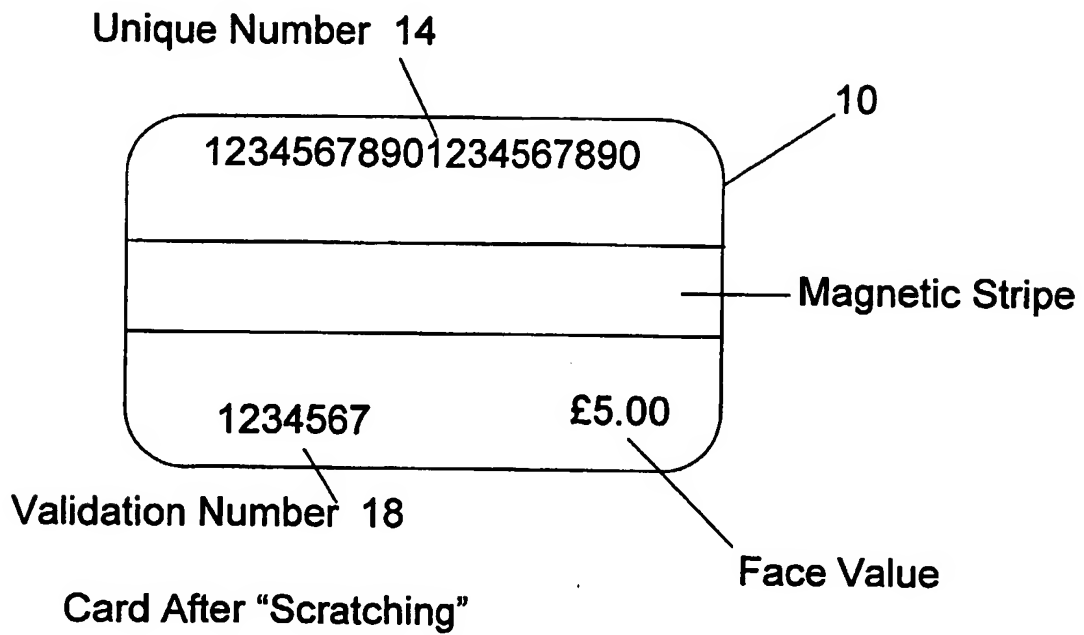
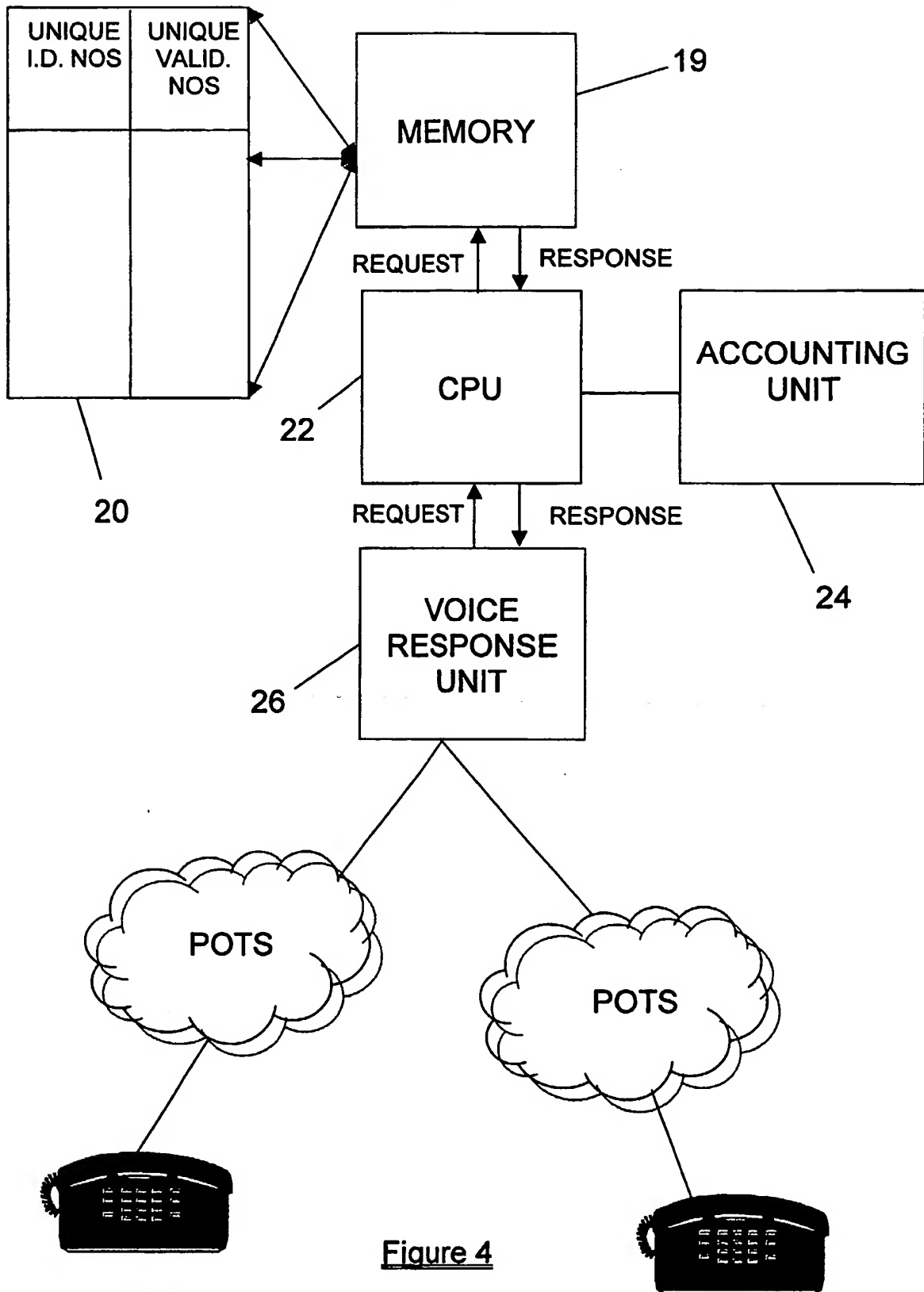


Figure 1Figure 2

20

IDENTIFICATION NUMBER	VALIDATION NUMBER	VALUE (£)
1234567890.....	123456	5

Figure 3

Figure 4

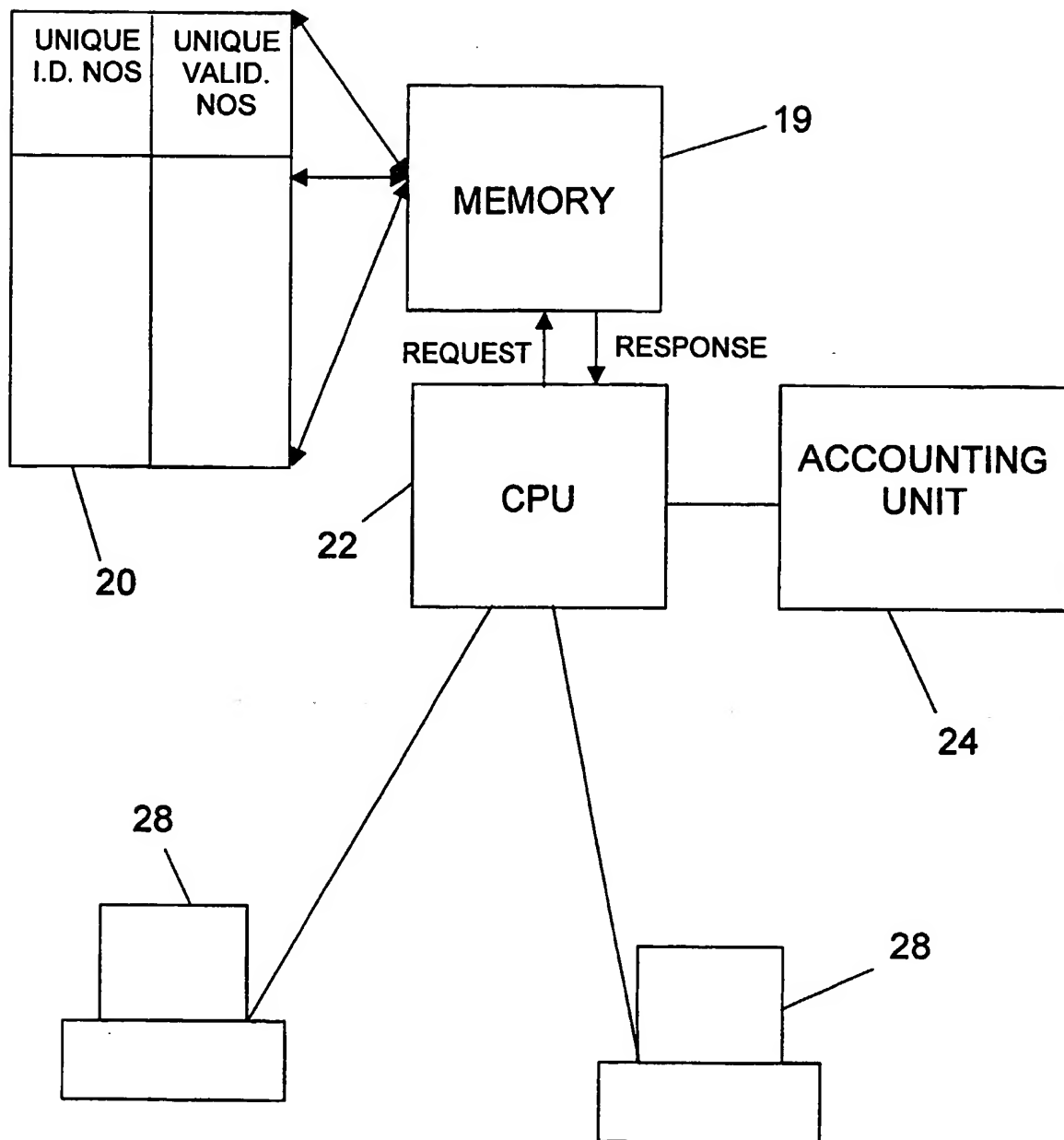


Figure 5

A CASH CARD AND A SYSTEM AND METHOD USING SUCH A
CARD

5 This invention relates to a cash card, in particular a face value scratch card, and a system and method for using such a card as a means for paying for goods and/or services.

10 Many methods of payment are available at present, including credit and debit cards. These are convenient and easy for customers to use and allow them to pay for goods and services either at a cash desk in a shop or equally over the telephone or internet.

15 In addition to well established methods of payment, a number of new methods are emerging, some of which relate to internet and digital payment services and others that are for more general use. One example is "Digicash", which is a means for paying for goods and services on the internet using an encrypted token. In this method, the buyer and seller are linked directly for the Digicash transaction. Settlement is a complex arrangement where the seller is
20 reimbursed by the Digicash service owner, who is paid by the customer using a credit or debit card or any other conventional payment transaction.

25 A problem with Digicash is, however, that it is anticipated that only a small number of consumers will use the service. This is due to the underlying perception that transactions on the internet are inherently insecure, because given time and resources is it generally possible to crack any practical cipher code. Un-crackable codes are of course possible at present, but suffer from

disadvantages that make them unusable for practical applications. A further disadvantage is that the Digicash system is dependent on the customer having some form of bank or credit card account. Many people, however, do not have access to this type of facility and so are excluded from internet or digital shopping.

An alternative system that is at a relatively early stage of development is known as Mondex, in which a smart card is loaded with encrypted information from an owner's bank account, which information is essentially a credit from the owner's bank account and represents a cash amount. The owner can then use the Mondex smart card bearing the information as if it were cash, at retail outlets that have card readers capable of reading the Mondex card.

Early indications suggest that the Mondex system is moderately successful. A disadvantage is, however, that to make its implementation widespread, it is necessary for a substantial investment in technology, both for smart cards and terminal equipment. At present, there is no drive to make the necessary investment and so the availability of Mondex is limited. In addition, as with Digicash, the Mondex system is dependent on the customer having some form of bank or credit card account. However, as noted above, many people do not have access to these.

An object of the present invention is to provide a system and method of non-cash payment that is simple and can be used widely by consumers, regardless of whether or not they have a credit card or a bank account.

According to one aspect of the present invention there is provided a cash card

that represents a cash amount, wherein the card bears a unique identification number that is concealed by a removable layer and a unique validation number that is concealed by a removable layer.

- 5 An advantage of this is that customers can buy the card and use it to purchase goods and services in the same way as if they were using money and without the need for a bank or credit card account. To do so, the unique number is exposed by removing the removable layer, which unique number can be verified by the goods or service provider to confirm that the card is authentic.
- 10 The goods or services provider settles payment with the provider of the card at a later time.

- The removable layer that covers the unique identification number may be removed by scratching it from the card. The removable layer that covers the
- 15 unique validation number may be removed by scratching it from the card. In either case, the removable layer may comprise a thin layer of aluminium.

- Preferably, the validation number is generated using the unique identification number. The validation number may be generated using a one time pad.

20

- According to another aspect of the present invention, there is provided a cash card authentication system comprising a plurality of cash cards that are each representative of a money amount, wherein each card bears a unique identification number that is concealed by a removable layer and a central
- 25 facility that includes a record of each unique identification number, thereby to provide a means for authenticating each card, when the removable layer is removed to expose the unique identification number.

The card may be a scratch card, wherein the removable layer that covers the unique identification number can be removed by scratching it from the card. The removable layer may comprise a thin layer of aluminium.

5

Preferably, the card bears a unique validation number for allowing the card holder to validate that the goods or service provider is able to exchange the card for goods or services, wherein the unique validation number is concealed by a removable layer. The card may be a scratch card, wherein the removable layer
10 that covers the unique validation number can be removed by scratching it from the card. The validation number may be generated using the unique identification number. The validation number may be generated using a one time pad.

15 Preferably, an accounting facility is provided to settle payment with goods and services providers.

According to yet another aspect of the present invention, there is provided a cash card security and authentication system comprising:

20

a plurality of cash cards that are each representative of a cash amount, wherein each card bears a unique identification number that is concealed by a removable layer;

means for entering a unique number into a computer system when the removable layer is removed to expose the unique identification number;

25

a central facility, remote from the means for entering the unique number, with a memory that includes a record of each unique identification number and a data processor that is operable to search the memory for the entered unique

number,

means for transmitting the entered unique identification number to the data processor, the data processor being operable to search the memory on receipt of the unique number,

5 means for generating a signal indicative of the authenticity of the card, when there is a match between the entered number and a number listed in the memory, thereby to provide a means for authenticating each card.

Preferably, the card bears a unique validation number for allowing the card
10 holder to validate that the goods or service provider is able to exchange the card for goods or services, wherein the unique validation number is concealed by a removable layer. The card may be a scratch card, wherein the removable layer that covers the unique validation number can be removed by scratching it from the card. The validation number may be generated using the unique
15 identification number. The validation number may be generated using a one time pad.

An automated voice response unit may be connected to the data processor, the automated voice response unit being operable to generate a voice message
20 indicative of the authenticity of the card, when there is a match between the entered number and a number listed in the memory.

Means may be provided for removing the number listed in the memory, when there is a match between it and the entered number. Means may be provided for
25 marking or highlighting a number or entry listed in the memory, when there is a match between it and the entered number. Means may be provided for generating a signal indicative of the invalidity of the card, when there is a match

between the entered number and a number that is marked or highlighted in the memory.

5 According to yet another aspect of the present invention, there is provided a cash card security and authentication system for authenticating a plurality of cash cards that are each representative of a cash amount and bear a unique identification number that is concealed by a removable layer, the system comprising:

10 means for entering a unique number into a computer system when the removable layer is removed to expose the unique identification number;

means for transmitting the entered unique identification number to a remote central facility that has a memory that includes a record of each unique identification number associated with the plurality of cash cards and a data processor that is operable to search the memory for the entered unique number and generate a signal indicative of the authenticity of the card when there is a match between the entered number and a number listed in the memory, and

15 means for receiving the signal indicative of the authenticity of the card, thereby to provide a means for authenticating each card.

20 Preferably, the system further includes means for receiving and displaying a unique validation code associated with the card.

According to yet a further aspect of the present invention, there is provided a payment method comprising:

25 providing a card that is representative of a cash amount, wherein the card bears a unique identification number that is concealed by a removable layer;

removing the removable layer to expose the unique identification

number, and

authenticating the card by checking the validity of the unique identification number with a central data facility that includes a record of authentic such unique identification numbers.

5

Preferably, the method further involves removing the unique identification number from the record of authentic such unique identification numbers in the central facility, when the unique identification number has been authenticated. An advantage of this is that a card bearing a unique identification number can
10 be used only once. After the identification number is removed from the record in the central facility, subsequent attempts to use the card cannot be authenticated. Alternatively, the method may involve marking or highlighting the unique identification in the record of authentic, when the unique identification number has been authenticated.

15

According to a still further aspect of the present invention, there is provided a payment method that uses a cash card that is representative of a cash amount, wherein the card bears a unique identification number that is concealed by a removable layer, the method comprising:

20

receiving the unique identification number when it is exposed,
authenticating the card by checking the validity of the unique number with a central facility that includes a record of authentic such unique identification numbers, and

25

on authentication of the card, accepting the card as at least part payment for goods or services.

Various aspects of the invention will now be described, by way of example

only, and with reference to the following drawings, of which:

Figure 1 is an example of a face value scratch card in which card information is obscured with removable opaque surfaces;

5 Figure 2 is an example of the face value card of Figure 1, in which the removable opaque surfaces are removed;

Figure 3 is an example of a database that includes identification and associated validation numbers;

Figure 4 is a block diagram of a first payment system that uses the card of Figures 1 and 2, and

10 Figure 5 is a block diagram of a second payment system.

Figure 1 shows a face value scratch card 10 that is representative of a cash amount, in this case £5.00, which amount is written on the card 10 in human readable text. At an upper portion of the scratch card 10, there is provided a
15 unique identification number that is concealed by an opaque surface 12, which can be removed, typically by scratching, to expose the unique number as and when desired by the user. Figure 2 shows a card 10 in which the unique identification number 14 is exposed, in this case 12345678901234567890. The unique identification number 14 for each card 10 is generated at random and
20 typically includes a code that is indicative of the cash value of the card.

Also provided on the card 10 is a unique validation number. As with the unique identification number 14, this is concealed by an opaque surface 16 that can be removed, again typically by scratching, to expose the validation number as and
25 when desired by the user. Figure 2 shows a card 10 in which the unique validation number 18 is exposed, in this case 123456.

The validation number 18 is typically generated using the unique identification number 14 as a cipher seed. For example, the validation number 18 can be generated using a one-time pad. In this method, the coding is only ever used once so that even if an attack were made and the code cracked it is of no use as
5 it is not used again. This method is well known and described in an article titled "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications" by J. Amer, Inst. Elec. Eng., vol. 45. Pages 109-115, 1926.

10 In order to use a one time pad for encoding a message the key code must be longer than the message. For example, if a one time pad of 1 3 5 2 17 5 9 10 8 20 1 6 were used to code a message "TORATORATORA", the alphabet would be stepped through as follows:

To T add 1 to get the next letter in the alphabet to become U,
15 To O step forward 3 letters in the alphabet to get R and so on.

The resulting coded message is "URWCKTAKBISG", with the original and the coded message being related only through the one time pad. Provided a copy of the pad is available, discovering the original message is simply a matter of subtracting the pad numbers to find the original letters. However, in the
20 absence of the pad, it is not possible to decode the message.

In order to construct a series of one time pads, there are certain mathematical rules that should be followed:

1. Each pad must have more bits than that of a character, e.g. at least 8
25 bits for ASCII.
2. Each pad must be completely different from the ones before it.

3. Each pad should be a function of a single changing variable that authorised parties can keep track of.

Using modulo arithmetic these characteristics can be satisfied. For example, using the "mod" allows a one time pad to operate as follows: If p and q are constants, prime and of size larger than 8 bits, the following equation can be used: $\text{pad} = p^n \bmod q$, where n is the n^{th} character of the message. To avoid pads of 0's, p must be larger than q , otherwise $\text{pad} = p^1 \bmod q = 0$. Similarly, n should not be set to 0. If these rules are met, a pseudo random number is generated having bits that can be either added or subtracted, (or any other function performed) on each character of the message. If exclusive OR (XOR - \oplus) is used, the number of bits remains the same and the repetition of the XOR gives the original message, i.e. $A \oplus B = C$, $C \oplus B = A$. Thus, $\text{msg} \oplus \text{Pad} = \text{cyphmsg}$ and $\text{cyphmsg} \oplus \text{pad} = \text{msg}$. This particular method of encryption is called a hash algorithm, where two elements are combined to form a third unique element.

In the present example, the "message" to be coded using a one time pad is the unique identification number 14. The resultant coded message is then used as the unique validation number 18.

Generation of the unique identification and validation numbers 14 and 18 respectively is done when the cards are manufactured. All the unique identification numbers 14 applied to the cards are stored in a database 20 in a central data facility 22, as shown in Figure 3. The central database 20 is typically provided and maintained by a trusted third party. Also stored with the unique identification numbers 14 are either the corresponding validation numbers 18 or the one time pad that was used to generate the corresponding

validation number 18. An advantage of storing the one time pad as opposed to the validation number 18 itself is that the validation number 18 is not stored in clear text, other than on the card on which it is printed. Optionally stored with the identification and validation numbers 14 and 18 respectively is an indication
5 of the cash value of each card 10. This is not, however, essential when the identification number 14 includes a code that is indicative of the cash value.

The cards 10 bearing the unique numbers are sold for the cash value indicated on the card 10. Hence, the card 10 of Figures 1 and 2 would be sold for £5.
10 The cards 10 can be exchanged for goods and services provided by goods and service vendors who have agreed to accept the cards 10 as payment, provided the unique identification number 14 on the card 10 is authenticated by the trusted third party. Payment is settled by the provider of the cards 10, which may be the trusted third party that maintains the central data facility or indeed
15 another party.

Figure 4 shows a system that allows a plurality of vendors to authenticate the face value cards 10 of Figures 1 and 2. This system includes a central data facility, which has a memory 19 that includes the database 20 that stores all of
20 the unique identification number 14 and the validation numbers 18 or one time pads, as appropriate. Connected to the memory 19 is a data processor 22 that is in turn connected to each of an accounting unit 24, which stores and processes each of the participating vendor's accounts, and an automated voice response unit 26. The technology for implementing the automated voice response unit 26
25 is well known and so will not be described here in detail. As is standard, the automated voice response unit 26 can be accessed by dialling a pre-determined telephone number.

The voice response unit 26 is adapted to request a vendor to identify a card 10 identification number 14 and transmit the identified number to the data processor 22, which is operable to search the database 20 for a match. If there is a match, a positive return signal indicative of the authenticity of the identification number 14 is generated by the processor 22 and sent to the automated voice response unit 26. Also generated and sent to the unit 26 is an indication of the validation number 18 associated with the identification number 14. This is done either by extracting the validation number 18 from the database 20 or by using the one-time pad stored in the database 20 to generate the validation number 18. At the same time, the unique identification number 14 recorded in the database 20 is deleted or suitably marked or highlighted by the processor to prevent it from being used again. In addition, a signal is sent to the accounting processor 24 to credit the vendor's account by the cash value associated with the card 10.

Receipt of the positive return signal triggers the voice unit 26 to transmit an automated voice response notifying the vendor that the entered identification number 14 is valid. The response unit 26 also provides the vendor with the validation number 18 that corresponds to the identification number 14, which can be read out to the card user.

In the event that there is no match between the entered number and the numbers in the central database 20, a negative return signal is generated by the processor and sent to the automated voice response unit 26, in this case the signal indicating that the number is invalid. Receipt of the negative return signal triggers the voice unit 26 to transmit an automated voice response notifying the

vendor that the entered identification number 14 is invalid. In this case the transaction is terminated.

5 The system of Figure 4 can be used when a customer wishes to purchase something either in person at a point of sales terminal in a shop or by telephone. In the case of a telephone purchase, the user calls the vendor's tele-sales service, identifies the desired product or service and explains the proposed method of payment. The user then scratches off the opaque surface on his cash card 10 to expose the unique identification number 14, which he reads out to the
10 vendor, who records it. The vendor then dials the pre-determined telephone number to connect to the automated voice response unit.

Once connected, the voice response unit 26 asks the vendor to read out the unique identification number 14. This number is then recorded and the
15 database 20 is searched to identify whether there is a match between the received identification number 14 and any of the recorded unique identification numbers 14. If there is, an automated voice response is provided notifying the vendor that the number is valid. The unique number 14 then either deleted from the database 20 or the database 20 is marked in some way to show that the
20 number 14 has been used. This confirms for the vendor that the card 10 is authentic and that payment for the goods requested will be settled by the card provider. The response unit 26 also provides the vendor with the validation number 18 that corresponds to the identification number 14. This is then read out to the card user, who can check the number with that on the card 10. If the
25 validation number 18 is correct, the user has confirmation that the vendor is party to the overall system. This provides the user with security.

In the event that the returned validation number 18 is not correct, there are several possible explanations, including:

(a) the validation number 18 may be incorrectly printed on the scratch card 10;

5 (b) the validation number 18 could have been corrupted in retrieval and or communications;

(c) the scratch card 10 could be a forgery;

(d) the vendor may not be authorised.

10 In the case of (a) and (b), if the vendor is bone fide, the unique number 14 on the card 10 will have been used and is no longer valid. However, until the validation number 18 is received the transaction may not be assumed complete and the card holder has no positive assurance that the remote organisation is bone fide. In this case, as in the case of (d), the holder has to take action that
15 seems appropriate at the time. For example, the card holder may take the matter up with the card supplier by reporting the error. In this case the party running the system could check to see whether the vendor is authorised and if the unique card number 14 has been marked as having been used. If the vendor is authorised the card holder is then provided with a degree of assurance.

20

An alternative approach would be to try an alternative supplier with the same card 10. If, in this second or subsequent attempt, the unique number 14 results in a returned validation code 18 that matches the code on the card 10, then this confirms that the second supplier is bone fide and the first was bogus. If in this
25 second attempt the number is refused, this suggests that the original company contacted was in fact bone fide and they may provide services. It should, however, be noted that the refusal of the card 10 in a second attempt is not

absolute confirmation that the original company was bone fide, because the unique number 14 (which of course is given to the original company) could have been used by the original company to purchase goods or services from an authorised vendor, in which case the card 10 could not be used by the actual card holder. In view of this, card holders will be encouraged to notify the card supplier of bogus vendors or problems with validation number matching as soon as possible, so that the integrity of the system can be maintained.

When the identification and validation numbers 14 and 18 respectively are correctly authenticated, the transaction is completed in the same manner as for a credit card transaction, with the card holder being sent the goods requested and the vendor settling payment for the goods with a trusted third party. If the goods and services ordered do not arrive, the holder can contact the card issuer for a refund or advice on other alternatives. This provides the card holder with the assurance that his transaction will be honoured as the vendor has been credited against the unique number 14. Where the goods and services still do not arrive after a reasonable delivery time interval, then the card holder can expect a refund from the card supplier, provided certain criteria are met.

As an alternative to the system of Figure 4, rather than reading the unique identification number 14 into a voice response unit, a pc or other electronic terminal could be provided with software for sending a message to the central facility. A suitable example is shown in Figure 5, in which each of the co-operating vendors has a sales terminal 28 that has dedicated scratch card computer software installed on it and is connected, typically via the POTS, to the central data facility. In this case, when a vendor wishes to authenticate a unique identification number 14, the number is merely typed into a data entry

field in the sales terminal 28 and an electronic message requesting authentication is sent to the central data facility. As before, when the request signal is received, the database 20 is searched to identify whether the entered unique identification number 14 is listed. If it is, a message is returned to the sales terminal authenticating the unique identification number 14 and the vendor's account is credited by the cash value associated with the card 10. Receipt of the authentication signal confirms for the vendor that the card 10 is valid. If the entered number 14 is not matched with an identification number in the database 20, a message is returned to the sales terminal indicating that the unique identification number 14 is invalid. When this happens, the transaction is terminated.

At the same time as returning the confirmation message, the central data facility sends the validation number 18 that corresponds to the identification number 14 to the sales terminal 28. This is presented on the screen of the sales terminal 28 so that the sales person can read that validation number 18 out to the customer, who then exposes the validation number 18 on their card 10 and checks if it is the same as that provided by the sales person. If it is, the user is provided with confirmation that the seller is an authorised seller. In this way, there is a two level authentication process for providing a security for firstly the sales person and secondly the customer.

In addition, or as an alternative, to the system of Figure 5, the vendor may provide a web site or interactive television or digital site that includes software for allowing a consumer to purchase goods or services therefrom using the cards 10 of Figures 1 and 2. In this case the software is operable to provide a purchase page having a data entry field that allows a user to enter the unique

identification number 14 of their card 10 in the same way as would be done for a credit card. Once the card identification number 14 is entered, the authentication process is substantially as described in relation to Figure 5.

5 The card 10 of Figures 1 and 2 may optionally be provided with a magnetic strip that carries a machine-readable version of the unique code, which machine-readable code is perfectly encrypted. The use of such a strip, however, does not offer the user the assurance that no one else knows the unique number and may be regarded as less secure.

10

Whilst in the specific examples described the unique identification number 14 is in human readable form, this number could be provided in a coded format, for example a bar code, that can be read using equipment provided at retailer's premises or even with a user's pc. In this case, rather than reading the card 10
15 visually and entering the read identification number 14 manually, the bar code would be scanned and the number automatically entered by the scanning equipment.

20

In addition, although the card 10 shown in Figures 1 and 2 only bears a single unique identification number 14, each card 10 could carry a plurality of such numbers, each being associated with a pre-determined cash amount. In this case, each of the identification numbers 14 is concealed by a removable surface and each is separately exposable and usable by the card holder to purchase goods and services.

25

In order to limit the number of unique identification numbers 14 that have to be stored in the central data facility, each cash card 10 may be set to be valid only

for a pre-determined period, for example six months. After expiry of that period, the unique identification number 14 stored in the database 20 would either be removed or marked to show that it has passed its expiry date. In this case, the card 10 would not be authenticated and any transaction would be terminated.

The security of the system described herein is provided by requirement that the cash cards 10 are authenticated using the unique identification number 14 prior to a transaction. As will be appreciated, the level of security on an unused card itself is zero, because anyone finding and using the card 10 would be in the same position as they would be had they found cash.

A skilled person will appreciate that variations of the disclosed arrangements are possible without departing from the invention. Accordingly, the above description of several embodiments is made by way of example and not for the purposes of limitation. It will be clear to the skilled person that minor modifications can be made without significant changes to the operation described above.

Claims

1. A cash card that represents a cash amount, wherein the card bears a unique identification number that is concealed by a removable layer and a unique validation number that is also concealed by a removable layer.
5
2. A cash card as claimed in claim 1, wherein the removable layer that covers the unique identification number is removable by scratching it from the card.
- 10 3. A cash card as claimed in claim 1 or claim 2, wherein the removable layer that covers the unique validation number is removable by scratching it from the card.
- 15 4. A cash card as claimed in any of the preceding claims, wherein the validation number is generated using the unique identification number.
5. A cash card as claimed in any one of the preceding claims, wherein the validation number is generated using a one time pad.
- 20 6. A cash card security and authentication system for authenticating a plurality of cash cards that are each representative of a cash amount and each bear a unique identification number that is concealed by a removable layer, the system comprising:
means for entering an identification number into a computer system
25 when the removable layer is removed to expose the unique identification number;
a central facility, remote from the means for entering the unique number,

with a memory that includes a record of each unique identification number and a data processor that is operable to search the memory for the entered unique number;

5 means for transmitting the entered unique identification number to the data processor, the data processor being operable to search the memory on receipt of the unique number, and

means for generating a signal indicative of the authenticity of the card, when there is a match between the entered number and a number listed in the memory, thereby to provide a means for authenticating each card.

10

7. A system as claimed in claim 6, wherein the removable layer that covers the unique identification number is removable by scratching it from the card.

15

8. A system as claimed in claim 6 or claim 7, wherein the card bears a unique validation number, the unique validation number being concealed by a removable layer.

20

9. A system as claimed in claim 8, wherein the removable layer that covers the unique validation number is removable by scratching it from the card.

10. A system as claimed in claim 8 or claim 9, wherein the validation number is generated using the unique identification number.

25

11. A system as claimed in any one of the claims 8 to 10, wherein the validation number is generated using a one time pad.

12. A system as claimed in any one of claims 6 to 11, wherein connected to the

data processor is an automated voice response unit that is operable to generate a voice message indicative of the authenticity of the card, when there is a match between the entered number and a number listed in the memory.

5

13. A system as claimed in any one of claims 6 to 12, wherein means are provided for removing the number listed in the memory, when there is a match between it and the entered number.

10

14. A system as claimed in any one of claims 6 to 12, wherein means are provided for marking or highlighting a number or entry listed in the memory, when there is a match between it and the entered number.

15

15. A system as claimed in claim 14, comprising means for generating a signal indicative of the invalidity of the card, when there is a match between the entered number and a number that is marked or highlighted in the memory.

20

16. A cash card security and authentication system for authenticating a plurality of cash cards that are each representative of a cash amount and bear a unique identification number that is concealed by a removable layer, the system comprising:

means for entering a unique number into a computer system when the removable layer is removed to expose the unique identification number;

25

means for transmitting the entered unique identification number to a remote central facility that has a memory that includes a record of each unique identification number associated with the plurality of cash cards and a data processor that is operable to search the memory for the entered unique number

and generate a signal indicative of the authenticity of the card when there is a match between the entered number and a number listed in the memory, and

means for receiving the signal indicative of the authenticity of the card, thereby to provide a means for authenticating each card.

5

17. A system as claimed in claim 16, comprising means for receiving and displaying a unique validation code associated with the card.

10

18. A payment method comprising providing a card that is representative of a cash amount, wherein the card bears a unique identification number that is concealed by a removable layer; removing the removable layer to expose the unique identification number, and authenticating the card by checking the validity of the unique identification number with a central facility that includes a record of authentic such unique identification numbers.

15

19. A payment method as claimed in claim 18 further involving removing the unique identification number from the record of authentic such unique identification numbers in the central facility, when the unique identification number has been authenticated.

20

20. A payment method as claimed in claim 18 further involving marking or highlighting the unique identification in the record of authentic numbers, when the unique identification number has been authenticated.

25

21. A payment method that uses a cash card that is representative of a cash amount, wherein the card bears a unique identification number that is concealed by a removable layer, the method comprising receiving the

unique identification number when it is exposed; authenticating the card by checking the validity of the unique number with a central facility that includes a record of authentic such unique identification numbers, and on authentication of the card, accepting the card as at least part payment for goods or services.



INVESTOR IN PEOPLE

Application No: GB 0030056.6
Claims searched: 1-21

Examiner: Graham Russell
Date of search: 11 July 2001

Patents Act 1977 Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:
UK Cl (Ed.S):
Int Cl (Ed.7): B42D 15/10; G06K 19/00
Other: Online: EPODOC, JAPIO, WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	GB 2314527 A (TRANSFER TECHNOLOGIES) see Figs 1-3 & page 7 lines 5-20	1-3
X	GB 2252270 A (WREN-HILTON) see page 12 line 1 - page 17 line 13	6,7,16, 18,21
X	WO 98/43825 A1 (ITTAH) see abstract and WPI abstract Acc No 1998-542519 [46]	1-3
X	US 5577109 (CALL PROCESSING) see column 3 line 55 - column 4 line 65	6,7,16, 18,21

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.